Amendment to specification under Article 34 of PCT

Paragraph [0007] on page 2 to page 3, paragraph [0011] on page 4, and paragraph [0012] on page 4 to page 5 of the specification have been amended in accordance with Article 34 of PCT. (Note: the other paragraphs have not been amended.)

Please prepare and file a necessary document.

The amended paragraphs [0007], [0011], and [0012] are as follows:

[0007]

In order to solve the above problems, one aspect of the present invention relates an electronic device, comprising:

mounting means for loading a portable recording medium; and

encrypted information write means for writing encrypted information obtained by encrypting predetermined information using an electronic device unique key unique to the electronic device, and an electronic device unique key encrypted using a recording medium unique key unique to the recording medium, in the recording medium;

characterized by further comprising:

authentication means for authenticating medium identification information for identifying the recording medium, and device identification information for identifying the

electronic device, in the case where the recording medium is mounted on the mounting means;

key generating means for generating a common encryption key for encrypting or decrypting the electronic device unique key in accordance with the authentication result of the authentication means;

encrypted information read means for reading the encrypted information recorded in the recording medium, and the encrypted electronic device unique key;

acquiring means for forwarding the read electronic device unique key to a control portion for the recording medium, and acquiring the electronic device unique key encrypted by the common encryption key from the control portion, after the electronic device unique key is decrypted by the recording medium unique key in the control portion;

decryption execution means for decrypting the acquired electronic device unique key by the common encryption key, and executing the decryption of the encrypted information using the decrypted electronic device unique key; and

control means for setting the electronic device in usable mode in the case where the encrypted information is decrypted by the decryption execution means.

[0011]

In order to solve the above problems, another aspect of the present invention relates to a method of controlling an

electronic device comprising:

mounting means for loading a portable recording medium; and

encrypted information write means for writing encrypted information obtained by encrypting predetermined information using an electronic device unique key unique to the electronic device, and an electronic device unique key encrypted using a recording medium unique key unique to the recording medium, in the recording medium;

characterized by comprising the steps of:

authenticating medium identification information for identifying the recording medium, and device identification information for identifying the electronic device, in the case where the recording medium is mounted on the mounting means;

generating a common encryption key for encrypting or decrypting the electronic device unique key in accordance with the authentication result;

reading the encrypted information recorded in the recording medium, and the encrypted electronic device unique key;

forwarding the read electronic device unique key to a control portion for the recording medium, and acquiring the electronic device unique key encrypted by the common encryption key from the control portion, after the electronic device unique key is decrypted by the recording medium unique key in the control portion;

decrypting the acquired electronic device unique key by the common encryption key, and executing the decryption of the encrypted information using the decrypted electronic device unique key; and

setting the electronic device in usable mode in the case where the encrypted information is decrypted.

[0012]

In order to solve the above problems, yet another aspect of the present invention relates to a security program characterized in that a computer included in an electronic device comprising:

mounting means for loading a portable recording medium; and

encrypted information write means for writing encrypted information obtained by encrypting predetermined information using an electronic device unique key unique to the electronic device, and an electronic device unique key encrypted using a recording medium unique key unique to the recording medium, in the recording medium;

is caused to function as:

authenticating medium identification information for identifying the recording medium, and device identification information for identifying the electronic device, in the case where the recording medium is mounted on the mounting means;

generating a common encryption key for encrypting or

decrypting the electronic device unique key in accordance with the authentication result;

reading the encrypted information recorded in the recording medium, and the encrypted electronic device unique key;

forwarding the read electronic device unique key to a control portion for the recording medium, and acquiring the electronic device unique key encrypted by the common encryption key from the control portion, after the electronic device unique key is decrypted by the recording medium unique key in the control portion;

decrypting the acquired electronic device unique key by the common encryption key, and executing the decryption of the encrypted information using the decrypted electronic device unique key; and

setting the electronic device in usable mode in the case where the encrypted information is decrypted.

Amendment to claims under Article 34 of PCT

Claims 1, 5, and 6 in the claims have been amended in accordance with Article 34 of PCT. (Note: the other claims 2 to 4, and 7 have not been amended.)

Please prepare and file a necessary document.

The amended Claims 1, 5, and 6 are as follows:

1. An electronic device, comprising:

mounting means for loading a portable recording medium; and

encrypted information write means for writing encrypted information obtained by encrypting predetermined information using an electronic device unique key unique to the electronic device, and an electronic device unique key encrypted using a recording medium unique key unique to the recording medium, in the recording medium;

characterized by further comprising:

authentication means for authenticating medium identification information for identifying the recording medium, and device identification information for identifying the electronic device, in the case where the recording medium is mounted on the mounting means;

key generating means for generating a common encryption

key for encrypting or decrypting the electronic device unique key in accordance with the authentication result of the authentication means;

encrypted information read means for reading the encrypted information recorded in the recording medium, and the encrypted electronic device unique key;

acquiring means for forwarding the read electronic device unique key to a control portion for the recording medium, and acquiring the electronic device unique key encrypted by the common encryption key from the control portion, after the electronic device unique key is decrypted by the recording medium unique key in the control portion;

decryption execution means for decrypting the acquired electronic device unique key by the common encryption key, and executing the decryption of the encrypted information using the decrypted electronic device unique key; and

control means for setting the electronic device in usable mode in the case where the encrypted information is decrypted by the decryption execution means.

5. A method of controlling an electronic device comprising:

mounting means for loading a portable recording medium; and

encrypted information write means for writing encrypted information obtained by encrypting predetermined information

using an electronic device unique key unique to the electronic device, and an electronic device unique key encrypted using a recording medium unique key unique to the recording medium, in the recording medium;

characterized by comprising the steps of:

authenticating medium identification information for identifying the recording medium, and device identification information for identifying the electronic device, in the case where the recording medium is mounted on the mounting means;

generating a common encryption key for encrypting or decrypting the electronic device unique key in accordance with the authentication result;

reading the encrypted information recorded in the recording medium, and the encrypted electronic device unique key;

forwarding the read electronic device unique key to a control portion for the recording medium, and acquiring the electronic device unique key encrypted by the common encryption key from the control portion, after the electronic device unique key is decrypted by the recording medium unique key in the control portion;

decrypting the acquired electronic device unique key by the common encryption key, and executing the decryption of the encrypted information using the decrypted electronic device unique key; and

setting the electronic device in usable mode in the case

where the encrypted information is decrypted.

6. A security program characterized in that a computer included in an electronic device comprising:

mounting means for loading a portable recording medium; and

encrypted information write means for writing encrypted information obtained by encrypting predetermined information using an electronic device unique key unique to the electronic device, and an electronic device unique key encrypted using a recording medium unique key unique to the recording medium, in the recording medium;

is caused to function as:

authenticating medium identification information for identifying the recording medium, and device identification information for identifying the electronic device, in the case where the recording medium is mounted on the mounting means;

generating a common encryption key for encrypting or decrypting the electronic device unique key in accordance with the authentication result;

reading the encrypted information recorded in the recording medium, and the encrypted electronic device unique key;

forwarding the read electronic device unique key to a control portion for the recording medium, and acquiring the electronic device unique key encrypted by the common encryption

key from the control portion, after the electronic device unique key is decrypted by the recording medium unique key in the control portion;

decrypting the acquired electronic device unique key by the common encryption key, and executing the decryption of the encrypted information using the decrypted electronic device unique key; and

setting the electronic device in usable mode in the case where the encrypted information is decrypted.